DAVID M. BENNION (5664)
SCOTT S. BELL (10184)
PARSONS BEHLE & LATIMER
One Utah Center
201 South Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsimile: (801) 536-6111

ERIC J. AMDURSKY (*pro hac vice* application pending)
PETE SNOW (*pro hac vice* application pending)
O'MELVENY & MYERS LLP
2765 Sand Hill Road
Menlo Park, California 94010
Telephone (650) 473-2600
Facsimile: (650) 473-2601

*Attorneys for Plaintiff Fusion Multisystems, Inc., d/b/a Fusion-io*

**IN THE UNITED STATES DISTRICT COURT**
**DISTRICT OF UTAH, CENTRAL DIVISION**

| | |
|---|---|
| FUSION MULTISYSTEMS, INC. d/b/a FUSION-IO,<br>Plaintiff,<br>vs.<br>DONALD G. BASILE,<br>Defendant. | **MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT**<br>Case No. 2:09-CV-00426<br>Judge J. Thomas Greene |

Plaintiff Fusion Multisystems, Inc. d/b/a Fusion-io ("Fusion-io"), by and through its undersigned counsel, respectfully submits this Memorandum in Opposition to Defendant's Motion to Dismiss Plaintiff's Complaint.

## INTRODUCTION

Plaintiff Fusion Multisystems, Inc., doing business as Fusion-io ("Fusion-io"), has adequately alleged that defendant Donald G. Basile ("Basile") violated multiple subdivisions of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"), by removing information from Fusion-io's computers and keeping it for his own unfair gain. Basile does not dispute (and cannot dispute for purposes of this Rule 12(b)(6) motion) that, in fact, he removed the information from Fusion-io's computers. Instead, Basile simply argues that the CFAA does not prohibit his conduct. Basile is wrong, and his selective reading of the CFAA does not warrant dismissal under Rule 12(b)(6).

First, Fusion-io's Fifth Claim states a claim under 18 U.S.C. § 1030(a)(5)(A) based on the damage Basile caused by diverting virtually all e-mails that he sent and received as Fusion-io's Chief Executive Officer away from Fusion-io's e-mail servers. It is easy to lose sight of this claim in Basile's Motion because Basile essentially ignores it. Under the plain language of the statute – which prohibits the transmission of a command that causes damage (i.e., any impairment to the integrity or availability of data) without authorization to a protected computer – Basile's conduct was unlawful. By diverting his e-mails away from Fusion-io's computers, Basile impaired Fusion-io's ability to access and protect the information contained therein, which constitutes "damage" under the statute. That conclusion is supported by the decision of every court to consider the question in similar circumstances. Courts have uniformly held that an employee who destroys information on his employer's computers impairs the integrity or availability of information within the meaning of the CFAA. Thus, Basile's Motion should be denied as to Fusion-io's Fifth Claim.

Second, Fusion-io's Sixth and Seventh Claims each states a claim under 18 U.S.C. §§ 1030(a)(5)(B), (a)(5)(C), and (a)(2) based on Basile's access to Fusion-io's computers both for the purpose of diverting his Fusion-io e-mails and for copying and retaining other information from Fusion-io's computers. The bulk of Basile's argument is devoted to the question whether his *access* to Fusion-io's computers was without authorization or in excess of authorization within the meaning of the statute (a question that applies only to the Sixth and Seventh Claims – not the Fifth). Basile's Motion hides the ball on the relevant law, as he presents the minority interpretation of the CFAA's "authorized access" provisions as unassailable until page 11 of his Motion, when he finally admits there is contrary (and better) authority.

Significantly, every Circuit Court of Appeals to consider the question has held that when employees access their employers' computers intentionally to cause "damage" (as that term is defined in the statute), they are not "authorized" to do so within the meaning of the CFAA. The contrary district court decisions and law review article on which Basile relies would redefine "unauthorized access" to mean a "code-based restriction on access" instead of simply "access without permission." Nothing in the CFAA, however, supports such an interpretation. Indeed, it would be contrary to the plain language of the statute, ordinary principles of statutory interpretation, the Legislative History, the intent of Congress in enacting the CFAA, and the weight of judicial authority.

Finally, because Fusion-io has stated one or more valid causes of action under the CFAA, the Court has clear supplemental jurisdiction over Fusion-io's state law claims, and Basile's attempt to avoid a federal forum through his Motion fails. For all of the foregoing reasons, and as set forth in greater detail below, Basile's Motion to Dismiss should be denied.

## ARGUMENT

### A. Fusion-io's Fifth Claim States A Claim For Damage To Its Protected Computer Systems Based On Basile's Diversion Of His E-Mails Away From Fusion-io's E-Mail Servers.

The CFAA establishes, *inter alia*, a civil right of action against anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). "Damage" is a defined term under the statute that "means any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

Fusion-io has alleged each of the elements of a claim under Section 1030(a)(5)(A) in its Complaint. Fusion-io alleges: (a) its computers are "protected computers" within the meaning of the CFAA (Compl. ¶ 72); (b) Basile caused the transmission of a program, information, code or command that caused the diversion of his Fusion-io e-mails from Fusion-io's protected computers (Compl. ¶ 74); (c) Basile did so without Fusion-io's authorization (*id.*); (d) Basile knowingly did so for the purpose of impairing the integrity or availability of data or information on Fusion-io's protected computers (Compl. ¶ 75); and (e) Basile's conduct caused precisely such an impairment (*id.*). In short, Fusion-io alleges that Basile diverted all of his Fusion-io e-mails to his personal e-mail account and deprived Fusion-io of those e-mails, which impaired the integrity or availability of that information. Under the plain language of the statute, such impairment constitutes "damage" and, therefore, Fusion-io has stated a claim under Section 1030(a)(5)(A) of the CFAA.

### 1. Judicial Precedent Confirms That Actions By An Employee To Remove Information From His Employer's Computers Without Authorization Violates Section 1030(a)(5)(A).

Basile does not cite a single judicial decision in his discussion of Fusion-io's Fifth Claim for violation of Section 1030(a)(5)(A), presumably because he could find none. (*See* Memo. at 4-6.) Fusion-io similarly is unaware of any authorities that would support Basile's argument seeking dismissal. Every judicial decision to consider the issue in similar circumstances has supported Fusion-io's position. Fusion-io cited two of these authorities in support of its application for a preliminary injunction, but Basile ignores them in his discussion of Section 1030(a)(5)(A).[1]

In *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) ("*Citrin*"), the Seventh Circuit Court of Appeals held that the plaintiff-employer had stated a cause of action under Section 1030(a)(5)(A) based on the deletion of data by the defendant-employee in circumstances similar to those presented here. The defendant in that case, Jacob Citrin, was a former employee of the plaintiff, IAC. Before returning his laptop to IAC, Citrin "deleted all the data in it—not only the data that he had collected but also data that would have revealed to IAC improper conduct in which he had engaged before he quit." *Id.* at 419. The court in that case noted that, "[o]rdinarily, pressing the 'delete' key on a computer (or using a mouse click to

[1] In Sections C and D of his Motion, which relate to Fusion-io's Sixth and Seventh Claims under separate subdivisions of the CFAA, Basile cites several district court decisions that disagree with *Citrin's* interpretation of those subdivisions. It is important to note, however, that none of those decisions questions or disagrees with *Citrin's* interpretation of Section 1030(a)(5)(A). Thus, even if the Court were to follow the decisions cited by Basile – which, for the reasons set forth below, it should not – it should still follow *Citrin's* interpretation of Section 1030(a)(5)(A).

delete) does not affect the data sought to be deleted; it merely removes the index entry and pointers to the data file so that the file appears no longer to be there . . . [s]uch 'deleted files are easily recoverable." *Id.* "But Citrin loaded into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery." *Id.* "IAC had no copies of the files that Citrin erased." *Id.* Accordingly, the Seventh Circuit held that "the transmission of the secure-erasure program to the computer" constituted the transmission of a program, information, code, or command within the meaning of the CFAA § 1030(a)(5)(A) that caused "damage," i.e., "any impairment to the integrity or availability of data, a program, a system, or information." *Id.*

Another court reached a similar conclusion in *Arience Builders, Inc. v. Baltes*, 563 F. Supp. 2d 883 (N.D. Ill. 2008). In that case, the plaintiff similarly alleged that, "[a]t or just prior to the termination of his employment with Plaintiff, Defendant decided to go into business and/or compete with Plaintiff and Defendant first secretly and maliciously copied and converted Plaintiff's Proprietary Business Information on said laptop computer for his own use, and then deleted, or caused to be deleted, and intended to delete, Plaintiff's Proprietary Business information from said laptop computer." *Id.* at 884. The district court held that the plaintiff "sufficiently allege[d] a transmission under the CFAA," which was "more than enough" to state a claim. *Id.*

Basile does not cite any contrary judicial authority or offer any other plausible interpretation of Section 1030(a)(5)(A). Instead, Basile cites legislative history in support of his argument that Section 1030(a)(5)(A) supposedly "was intended to provide criminal penalties and civil liability for persons who send or download destructive viruses and worms to protected computers." (*See* Memo. at 5) Neither the statutory language nor the legislative history of the

CFAA, however, supports such a narrow construction. The stated purpose of the amendment was "to clarify and strengthen" the CFAA "[i]n light of rapid developments in computer technology . . . to ensure that novel forms of computer abuse are prohibited." S. Rep. 101-511 (1990), 1990 WL 201793, *1. Significantly, the Senate specifically understood and intended that the amendments should apply to corporate insiders: "We think it should be possible using Federal law, therefore, to prosecute a disgruntled employee who introduces a harmful program code . . ." *Id.* at *4.[2] Indeed, one of the decisions cited by Basile, *In re America Online, Inc.*, 168 F.Supp.2d 1359 (S.D. Fla. 2001), notes that the legislative history of a subsequent amendment to the CFAA "reinforces this conclusion, 'Specifically, as amended, subsection 1030(a)(5)(A) . . . would cover anyone who intentionally damages a computer, *regardless of whether they were an outsider or an insider or otherwise authorized to access the computer*.'" *Id.* at 1371 (quoting S. Rep. 104-357, at 11, Aug. 27, 1996) (emphasis added).

*Citrin* and *Arience Builders* correctly interpreted Section 1030(a)(5)(A) to prohibit employees from causing the destruction of information on their employers' computers, and their reasoning is fully applicable here. Section 1030(a)(5)(A) prohibits any intentional impairment of integrity or availability of information or data, which, as alleged in Fusion-io's Complaint, was the inevitable result of Basile's actions in intentionally diverting the e-mails he sent and received as CEO of Fusion-io away from the company's computers. (Complaint ¶¶ 24-25.) Significantly, Basile could have forwarded his e-mails to a personal account in such a way that Fusion-io would have retained copies of them, and Fusion-io's e-mail system was set up that way by

[2] Basile argues that he was not "disgruntled" (*See* Memo. at 6), which is not a fact alleged in the Complaint. Even if it is assumed that Basile was more disloyal, conniving, and/or calculating than "disgruntled," however, there is no basis in the statute for exempting him from liability simply because he had a different wrongful motive than the one specifically suggested in the legislative history.

default. (*Id.*) Yet Basile deliberately overrode that default setting so that Fusion-io's e-mail servers would not retain any copy. (*Id.*) There was no reason for Basile to do that, other than to impair their availability to Fusion-io, which is the definition of intentional "damage" under the CFAA.

Basile does not dispute – and cannot dispute for purposes of this Motion – that he intentionally diverted his Fusion-io e-mails away from the company's servers for the purpose of impairing the availability of those e-mails to Fusion-io. He also does not dispute that Fusion-io was deprived of the information contained in the e-mails as a result. Instead, Basile argues that he was "authorized" to do so because "[a]t the time the emails were allegedly forwarded, Basile was Fusion's CEO." (*See* Memo. at 4.) In other words, Basile appears to argue that, as CEO, he was above the law and could "authorize" himself to steal Fusion-io's confidential information for use in subsequent employment with a competitor. Fusion-io is confident that Basile cannot prove such an assertion. The facts will show that Basile's authority as CEO was limited to acting in the best interests of the company – and taking his e-mails from the company was contrary to those interests. For present purposes, however, Fusion-io need not establish those facts; it suffices that Fusion-io has alleged that, even as CEO, Basile was not authorized to engage in that conduct. (Compl. ¶ 74.)[3]

Basile also argues that "there are no allegations that Basile violated any company email retention policy or rule; that Basile took steps to try and conceal his conduct from others; or that

[3] In a footnote, Basile argues that the allegations of the Complaint are contradicted by the declaration of Fusion-io's Information Technology Manager, who assisted Basile in causing the diversion of his e-mails in such a way that Fusion-io retained no access to them. Basile is correct that the declaration cannot be considered for purposes of this Motion, but it only supports Fusion-io's claim. Basile's actions did not become "authorized" simply because Basile directed a subordinate employee to help him cause damage within the meaning of the CFAA.

anyone objected to his alleged 'forward only' method." (*See* Memo. at 4-5.) These arguments are irrelevant because Section 1030(a)(5)(A) does not require any of those things. The absence of a policy does not constitute affirmative *authorization*. The Company does not have a written policy prohibiting employees from stealing office supplies either, but that does not mean employees are authorized to do so. Similarly, whether or not Basile took steps to conceal his conduct, he certainly did not inform the Company's Board of Directors (to which he reported) of his conduct or request authorization for it. Finally, Basile's argument that no one objected to his conduct reflects nothing more than the fact that, as alleged in the Complaint, the Company was not aware of it. (Compl. ¶ 74.) If Basile had informed the Board of Directors what he was doing – which he had an obligation, but failed, to do – the Board would have objected. At a minimum, however, the Company did not "authorize" Basile's conduct. (*Id.*) Thus, Fusion-io has properly stated a claim under Section 1030(a)(5)(A).

### 2. Even The Law Review Article On Which Basile Relies In Support Of His Argument On Fusion-io's Sixth And Seventh Claims Recognizes The Validity Of Fusion-io's Fifth Claim.

Basile's Motion relies, in part, on a law review article: Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L.Rev. 1596. (*See* Memo at 12-13.) As discussed below, that article's discussion of "unauthorized access" statutes (such as 18 U.S.C. §§ 1030(a)(2) and (a)(5)(B) and (C)) is contrary to uniform Circuit Court authority and should not be followed. Nevertheless, it is worth noting that even that article supports Fusion-io's Fifth Claim under Section 1030(a)(5)(A). Mr. Kerr states:

> For example, in Fugarino, the defendant's harmful act was interfering with his employer's business; by deleting his

> employer's files, Fugarino ensured that the business and its employees would be unable to exercise their usual privileges of using the files. The Fugarino court apparently reasoned that this was an unauthorized access because the destruction was unauthorized, and to destroy the files, Fugarino had to access the computer that hosted them. But Fugarino's crime was not really unauthorized access; it was willful destruction of his employer's files with the intent to deprive the employer of their use.
>
> Congress enacted an intentional damage statute to complement the federal unauthorized access statute in 1986. Codified at 18 U.S.C. § 1030(a)(5), this statute in its current form states that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" commits a federal felony. . . . States should enact similar provisions, and courts should interpret unauthorized access statutes while mindful of the existence of computer damage statutes. *Id.* at 1661-62 (citing *Fugarino v. State*, 243 Ga. App. 268 (2000)).

Fusion-io disagrees with much of what Mr. Kerr writes, including his critique of *Fugarino* and the false dichotomy Mr. Kerr creates between what he calls "unauthorized access statutes" (which include Fusion-io's Sixth and Seventh Claims) and "intentional damage statutes" (which include Fusion-io's Fifth Claim). Even Mr. Kerr concedes, however, that an employee's elimination of computer data that makes "the business and its employees . . . unable to exercise their usual privileges of using the files" constitutes a violation of Section 1030(a)(5)(A). Fusion-io does not suggest that this Court accept this interpretation of the law simply because Mr. Kerr says so. But when even academia's most staunch advocate for a narrow interpretation of the CFAA admits that Section 1030(a)(5)(A) prohibits the type of conduct alleged by Fusion-io in its Fifth Claim, it makes clear that there is no contrary argument.

In accordance with *Citrin*, *Arience Builders*, and the plain language of the statute, this Court should deny Basile's Motion to Dismiss Fusion-io's Fifth Claim. Fusion-io has properly alleged that Basile caused "any impairment to the integrity or availability of data . . . or information" – i.e., that he caused "damage" within the meaning of the statute – by diverting the e-mails he sent and received as CEO to his personal e-mail account and preventing Fusion-io's e-mail servers from retaining any copy of those e-mails for Fusion-io's uses.

### B. **Fusion-io's Sixth And Seventh Claims State Valid Claims For Access Without Authorization Or In Excess Of Authorization To Its Protected Computer Systems.**

Fusion-io's Sixth Claim is under 18 U.S.C. § 1030(a)(5)(B) and (C), which makes it unlawful to "intentionally access[] a protected computer without authorization, and as a result of such conduct, recklessly cause[] damage," or "intentionally access[] a protected computer without authorization, and as a result of such conduct, cause[] damage and loss." Fusion-io's Seventh Claim is under Section 1030(a)(2), which makes it unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer."

Basile's Motion to Dismiss is based on a single element of these two claims – whether Basile acted "without authorization" or whether he "exceed[ed] authorized access." Basile does not dispute that by diverting his e-mails and taking other information from Fusion-io's computers, he accessed Fusion-io's computers and obtained information. Basile also does not dispute that his actions intentionally caused statutorily-defined "damage" (i.e., the impairment of availability or integrity of data or information) by depriving Fusion-io of the information contained in the e-mails and the ability to safeguard it by exclusively maintaining the information in the company's protected computers. At a minimum, Basile does not dispute that these elements adequately are alleged in the Complaint. (Compl. ¶¶ 80-98.) Thus, like Basile, Fusion-io will focus on the question of authorization.

As Basile acknowledges, the term "without authorization" is not defined in the CFAA, but the term "exceeds authorized access" is defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Basile also appears to concede that "authorization" should be given its "ordinary meaning, i.e., 'the act of conferring authority; permission,'" (*see* Memo. at 6), although that concession is squarely at odds with his argument. Under the plain meaning of the statute, Basile was not authorized – i.e., given permission – to divert the e-mails he sent or received as CEO of Fusion-io, or other confidential and proprietary Fusion-io information, to his personal e-mail account or computer. Those actions impaired the availability and integrity of Fusion-io's information by removing it from Fusion-io's computers and, as Fusion-io has alleged, the company did not "authorize" Basile to engage in such conduct. Thus, Fusion-io adequately has stated its Sixth and Seventh Claims. As discussed further below, that straightforward conclusion is further supported by the weight of precedent, the legislative history of the statute, and Congress' purpose in enacting and amending the CFAA.

### 1. Despite The So-Called "Split Of Authority" On The Question, The Weight Of Precedent Compels The Conclusion That Employees Lack Authorization To Copy Or Destroy Information On Their Employers' Computers For Their Own Benefit Or To The Intentional Detriment Of Their Employers.

Basile correctly notes that the Tenth Circuit has not interpreted the word "authorization" as used in the CFAA, but he does not fairly set forth the competing viewpoints developed in other Circuits. Although a handful of district court decisions have gone Basile's way, the weight of authority (including all of the Circuit Court authority) has held that employers do not authorize employees' access to impair the availability or integrity of data or information on their computers. As these decisions persuasively explain, when employees intentionally cause "damage" within the meaning of the statute there is, at a minimum, a triable issue as to whether the employees accessed their employers' computers "without authorization" or "exceeded authorized access" to those computers.

### a. The Most Persuasive Authorities Confirm That Employees May Be Held Liable Under The CFAA For Accessing Their Employers' Computers Without Authorization Or In Excess Of Their Authorization.

At least four (and arguably five) Circuit Courts of Appeals have held that agents or employees preparing to engage in unfair competition with their principals or employers, or who seek to copy or destroy information for their own malicious ends, have accessed their employers' computers without authorization or in excess of their authorized access. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001) (affirming preliminary injunction under the CFAA against a consultant who "exceeded . . . authorization by providing proprietary information and know-how" to a competitor in violation of a confidentiality agreement); *P.C. Yonkers, Inc. v. Celebrations The Party & Seasonal Superstore, LLC*, 428 F.3d 504, 513 (3d Cir. 2005) (holding that a claim against an employee and consultant for unauthorized access "is cognizable under the statutory framework and language," but holding that the district court did not err in holding that plaintiffs had failed to adduce sufficient proof of a violation to merit preliminary injunctive relief); *Fiber Systems Int'l, Inc. v. Roehrs*, 470 F.3d 1150, 1171 (5th Cir. 2006) (vacating district court's order and directing it to enter judgment in plaintiff's favor on claim under Section 1030(a)(4), which prohibits access of a protected computer without authorization, against five former officers of the plaintiff who copied and deleted information from the plaintiff's computers); *International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (reversing district court's dismissal of claim under CFAA and holding that employee's actions in destroying information on his employer's computer was without authorization within the meaning of the CFAA); *see also Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 932 (9th Cir. 2004) (affirming judgment in favor of plaintiff on claim under CFAA where defendant's conduct included both using an employee of the plaintiff to download plaintiff's customer list and exploiting an uninstalled security patch to gain access to the plaintiff's source code). To Fusion-io's knowledge, there is no contrary Circuit Court authority, and certainly none is cited by Basile.[4]

These decisions thoroughly debunk Basile's characterization of the CFAA as simply applying to "computer hackers, or electronic trespassers," and make clear, instead, that it also applies to a company's employees. It may be true that, "the majority of CFAA cases still involve 'classic' hacking activities. However, the scope of its reach has been expanded over the last two decades. Employers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." *P.C. Yonkers*, 428 F.3d at 510 (citations and internal quotation marks omitted). "Such long-distance attacks [as transmitting a virus] can be more difficult to detect and thus to deter or punish than ones that have been made

[4] Basile relies entirely on published and unpublished district court authority, and at that level, some cases do support Basile's argument. Numerous district court cases, however, are in accord with the Circuit Court decisions cited above. *See, e.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000); *Pacific Aerospace & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188 (E.D. Wash. 2003); *ViChip Corp. v. Lee*, 438 F. Supp. 2d 1087 (N.D. Cal. 2006); *Nilfisk-Advance, Inc. v. Mitchell*, 2006 WL 827073 (W.D. Ark. 2006); *George S. May Int'l Co. v. Hostetler*, 2004 WL 1197395 (N.D. Ill. 2004); *HUB Group, Inc. v. Clancy*, 2006 WL 2008684 (E.D. Pa. 2006); *Int'l Sec. Mgmt. Group, Inc. v. Sawyer*, 2006 WL 1638537 (M.D. Tenn. 2006).

only by someone with physical access, usually an employee. The inside attack, however, while easier to detect may also be easier to accomplish. Congress was concerned with both types of attack: attacks by virus and worm writers, on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other." *Citrin*, 440 F.3d at 420.

These cases comport with common sense and the plain language of the CFAA. Employers do not grant their employees *carte blanche* to do whatever they want with the employers' computer systems. An employer may share its customer list with an employee so that the employee can call on a customer, but that does not mean the employee is authorized to copy the customer list to give to a competitor. An employer may give an employee the ability to edit computer files so that the employee can update them with relevant information, but that does not mean that the employee is authorized to delete all of the information contained in the files to disrupt the employer's business. In short, when an employee intentionally causes damage within the meaning of the CFAA (i.e., any impairment to the integrity or availability of data or information), it is no defense – particularly on a motion to dismiss – that the employee was "authorized" to do so. As Fusion-io has alleged, Basile diverted his Fusion-io e-mails and other computer data away from Fusion-io's computers, impairing the integrity or availability of that information. Fusion-io specifically has alleged that Basile did so without authorization or in excess of his authorization and, therefore, Fusion-io adequately has alleged its Sixth and Seventh Claims under the CFAA.

### b. The Contrary District Court Decisions On Which Basile Relies Are Based On An Interpretation Of The CFAA That Cannot Be Reconciled With The Statutory Language.

Notwithstanding the foregoing authorities, Basile is correct that several district court decisions have held, in effect, that employees cannot be held liable under the CFAA for accessing their employers' computers without authorization or in excess of authorization. (*See* Memo. at 6-10.)[5] Basile also relies heavily on Professor Orin S. Kerr's law review article that is discussed by several of those decisions, and which most clearly expresses the basis for their holdings. Professor Kerr offers his opinion as to how the CFAA should be interpreted: "Courts should distinguish between the two ways in which use of a computer may exceed the rights granted to a user. First, a user can violate a contractual agreement with the owner or operator of the computer. Second, a user can circumvent a code-based restriction on the user's privileges. In the first case, the use of the computer is unauthorized in the sense that it violates an implicit (and sometimes explicit) contract. . . . In the latter case, the use is unauthorized in the sense that it bypasses a code-based effort to limit the scope of the user's privileges." 78 N.Y.U. L.Rev 1596, 1599-1600. The latter interpretation manifests itself in the decisions on which Basile relies when he argues that the "CFAA . . . do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do [its] terms proscribe authorized access for unauthorized or illegitimate purposes." (Memo. at 6, quoting *Werner-Masuda*, 30 F. Supp. 2d at 499).

[5] Citing *Lockheed Martin Corp v. Speed*, 2006 WL 2683058 (M.D. Fla. 2006); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); *Brett Senior & Assocs. v. Fitzgerald*, 2007 WL 2043377 (E.D. Pa. 2007); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008); *In re America Online, Inc.*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001); *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593 (E.D. Va. 2005).

Professor Kerr "proposes that courts should reject contract-based notions of authorization, and instead limit the scope of unauthorized access statutes to cases involving the circumvention of code-based restrictions." Orin Kerr, 78 N.Y.U. L.Rev. at 1600. The primary problem with Professor Kerr's argument, however, is that it is not based on any attempt to determine what Congress actually intended in enacting the CFAA; instead, it is based on nothing more than Professor Kerr's own opinion of what ideal legislation would look like. Indeed, Professor Kerr admits that his ideal legislative solution does not necessarily reflect the current state of the law:

> One doctrinal objection to this proposal is that federal law arguably already attempts to protect these interests through prohibitions on "exceeding authorized access" to computers. As I mentioned earlier, the prohibition on exceeding authorized access appears to have been directed at *misuse* committed by insiders, those with preexisting rights and privileges. Precedent exists to support the view that this prohibition covers breach of contractual restrictions by otherwise-legitimate users.
>
> *Id.* at 1662 (emphasis added).

Professor Kerr nevertheless argues that the CFAA is susceptible to two interpretations and advocates for the more narrow one, which a few district courts have adopted. Faced with this split between numerous Circuit Court of Appeals and district court decisions holding that employees can violate the unauthorized access provisions of the CFAA, on the one hand, and several district court decisions and Professor Kerr's law review article claiming that employees cannot violate those provisions, on the other hand, this Court should resolve Basile's Motion as to Fusion-io's Sixth and Seventh Causes of Action using normal principles of statutory interpretation. As set forth below, those principles compel adoption of the view uniformly embraced by the Circuit Courts – and the denial of Basile's Motion in its entirety.

### 2. The Plain Language Of The Statute Compels The Conclusion That Employees Lack Authorization To Copy Or Destroy Information On Their Employers' Computers For Their Own Benefit Or To The Intentional Detriment Of Their Employers.

The Court's task of statutory interpretation necessarily begins with the statutory language itself. The statute defines "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The key term in interpreting that definition is "entitled." Black's Law Dictionary defines "entitle" as follows: "To grant a legal right to or qualify for." Bryan A. Garner, *Black's Law Dictionary* (8th Edition) at p. 573 (2004). Using that ordinary definition, the CFAA prohibits a person from "exceeding authorized access" by using "access to obtain or alter information in the computer that the accesser is not entitled" – i.e., does not have a legal right – "to so obtain or alter."

Thus understood, the CFAA's definition of "exceeding authorized access" is best interpreted as including situations where an employee exceeds authorized access by violating a contractual agreement with the owner of the computer. If the access violates any contractual duty or any duty imposed by law, the individual did not have a "legal right" to such access. The statute is not susceptible to the alternative interpretation that an employee exceeds authorized access only by bypassing a code-based restriction. Even if an employer gives an employee a password that grants access to its computers, the employee is not entitled – i.e., does not have a legal right – to obtain or alter information on the computers if doing so would violate a duty imposed by contract or law on the employee. The statute is unambiguous, and the Court should follow this plain-language interpretation.

The result is the same when interpreting the phrase "without authorization." That phrase is not defined by the CFAA, so Basile argues that it should be given its "ordinary meaning, i.e., 'the act of conferring authority; permission.'" (Memo at 6, citing *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 at *5.) Giving it that meaning, however, again leads to the conclusion that an employee accesses a computer "without authorization" when he or she does so in violation of any contractual or legal right of the employer. Employers do not confer authority or permission on employees to access employer computers to violate employer rights. By contrast, there is no way to interpret "without authorization" to mean "in violation of a code-based restriction." That is simply not the ordinary meaning of authorization. If Congress had intended such a narrow interpretation of the CFAA, it could have used that narrow language. Because the statute uses broader language that encompasses contractual and legal rights (as well as code-based restrictions), it should be given that effect.

Because the statutory language is unambiguous, this Court should hold that Basile was "without authorization" or "exceeded authorization" when he diverted Fusion-io's e-mails and other information in violation of his contractual and/or legal duties to Fusion-io not to impair the availability or integrity of Fusion-io's information – whether or not he circumvented any code-based restriction in doing so. "If the statute is clear and unambiguous, that is the end of the matter. There is no need to look beyond the plain meaning in order to derive the 'purpose' of the statute." *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1128-29 (W.D. Wash. 2000) (holding that under the plain language of the CFAA, employees who use their employer's computer systems to send trade secrets to a competitor act "without authorization" within the meaning of the statute). Thus, Basile's Motion should be denied.

### 3. The Legislative History Of The Statute And Ordinary Principles Of Statutory Interpretation Similarly Compel The Conclusion That Employees Lack Authorization To Copy Or Destroy Information On Their Employers' Computers For Their Own Benefit Or To The Intentional Detriment Of Their Employers.

If the language of the CFAA is ambiguous – that is, if it is susceptible to both of the interpretations above as Professor Kerr argues – the Court must then attempt to determine which of the interpretations Congress intended. That analysis leads to the same result: Congress specifically intended that the CFAA's provisions on unauthorized access would apply to employees of a company who cause statutorily-defined damage to its computers.

In support of his contrary argument, Basile relies upon *Shamrock Foods*, which analyzed the 1984 legislative history of the CFAA and concluded that "the committee report emphasized concerns about 'hackers' who 'trespass into' computers and the inability of 'password codes' to protect against the threat." 535 F. Supp. 2d at 965-66. Another of the district court decisions on which Basile relies similarly cites the 1990 legislative history for the proposition that, "a civil cause of action was created under the CFAA to redress damage and a loss as a result of serious computer abuse, such as transmission of computer 'viruses' and 'worms.'" *Werner-Masuda*, 390 F. Supp. 2d at 495-96.

The decisions relied upon by Basile, however, cite to the legislative history for earlier versions of the CFAA, as it existed in 1984 and 1990, which has little if any continuing vitality following subsequent amendments to the statute in 1996. As the Third Circuit noted, "the scope of [the CFAA's] reach has been expanded over the last two decades." *P.C. Yonkers*, 428 F.3d at 510. The 1996 legislative history to the CFAA confirms the statute's applicability to employees like Basile: "For example, individuals who intentionally break into, *or abuse their authority to use*, a computer and thereby obtain information of minimal value of $ 5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for *purposes of commercial advantage or private financial gain*, for the purposes of *committing any criminal or tortious act in violation* . . . of the laws of the United States or of any State, or if the value of the information obtained exceeds $ 5,000." *Shurgard*, 119 F. Supp. 2d at 1128-29 (emphasis in original; quoting S. Rep. No. 104-357, at 3 (1996)). The *Shurgard* court concluded: "This legislative history, although in reference to § 1030(a)(2), demonstrates the broad meaning and intended scope of the terms 'protected computer' and 'without authorization' that are also used in the other relevant sections. Finally, the report states the statute is intended to punish those who illegally use computers for commercial advantage. In sum, this passage makes clear that the CFAA was intended to encompass actions such as those allegedly undertaken by the present defendant. The legislative history of the CFAA comports with the plain meaning of the statute." *Id.* at 1129. Thus, the court held that the plaintiff adequately alleged claims against a former employee for violations of Sections 1030(a)(2)(C) and 1030(a)(5)(C), which Fusion-io has alleged in its Sixth and Seventh Causes of Action.

Additionally, it is a principle of federal law that courts "interpret federal statutes in light of the common law." *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) (interpreting the Stored Communications Act, the Wiretap Act, and the CFAA). As such, the courts in *Citrin* and *Shurgard* properly relied upon the Restatement (Second) of Agency § 112 in holding that the employees accessed their employers' computers without authorization. Neither Basile nor the decisions on which he relies suggest any other principle of common law that should be used to interpret the CFAA in Section 112's place. Instead, Basile notes that one district court refused to follow *Citrin* and *Shurgard* because under such an interpretation, "employers suddenly have a federal cause of action whenever employees access the company computer with 'adverse interests' and such action causes a statutorily recognized injury." (Memo. at 13-14, quoting *Lockheed Martin*, 2006 WL 2683058 at *7.) Although that court found that the breadth of the CFAA was "disconcerting," such results-based reasoning is no basis for interpreting the statute.

In accordance with the legislative history and the plain meaning of the statute, the Court should hold that Fusion-io has properly alleged its claims and deny Basile's Motion. Congress intended for the CFAA to be broadly applicable to insiders as well as outsiders, and there is no basis in the legislative history or the common law for any other interpretation.

### 4. A Contrary Interpretation Of The CFAA Would Lead To Absurd Results And Flout Congress' Intent In Enacting The CFAA To Provide Effective Protection Against Computer Crimes.

The authorities on which Basile relies reach the wrong result and, taken to their logical conclusions, would wholly undermine Congress' purpose in enacting (and subsequently broadening through amendments) the CFAA.

In *Shamrock Foods*, a case cited by Basile, the district court refused to follow the Circuit Court's interpretation of the CFAA in *Citrin* in part because, "[t]his case is also factually distinguishable from *Citrin*. Here, the information accessed . . . was not altered, damaged, or destroyed. Instead, it was allegedly used in an improper manner." 535 F. Supp. 2d at 967, n.11. If that is the limit of *Shamrock Foods'* holding, all of the cases on which Basile relies may be distinguished from the present matter. The cases cited by Basile did not deal with the situation presented in *Citrin*, *Arience Builders*, and here, where the defendant not only copied the plaintiff's information but also eliminated it from the plaintiff's computers so that the plaintiff would have no copy of it. Arguably, Basile's Motion could be denied on that basis.

Professor Kerr, however, more candidly admits that an interpretation of "unauthorized access" that excludes employees who copy information from their employers' computers would have more far-reaching effects. Professor Kerr begins with the situations presented here: a hypothetical "employee who wants to start a competing business" who copies his employer's files and another who "delet[es] some of his employer's important files," according to Professor Kerr, have not violated the CFAA because, as employees, they have not violated any code-based restriction on their conduct. Orin Kerr, 78 N.Y.U. L.Rev. at 1664. But Professor Kerr acknowledges he cannot stop there. For example, a person who launches a "denial-of-service" attack[6] on a company's website "will not itself constitute an unauthorized access crime. Sending the data to the computer does access the computer, but the access is not without authorization: The webserver has been configured to accept all web traffic requests, such that sending many requests will not circumvent any code-based restrictions." *Id.* at 1664-64. Indeed, Professor Kerr admits that even traditional transmission of a computer virus could escape sanction under his interpretation of the CFAA. *Id.* at 1665-66.

Any interpretation of the CFAA that would not clearly prohibit the transmission of viruses or the launching of denial-of-service attacks, like that posited by Professor Kerr and the district court decisions on which Basile relies, must be rejected. There can be no doubt that Congress intended the CFAA to prohibit such conduct. Under Basile's interpretation, if he had destroyed every single file on Fusion-io's computers and caused its website to be unusable by consumers, he would have been "authorized" to do so because he was an employee and he did

[6] A denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

not circumvent any code-based restriction. That cannot be the law. As alleged in the Complaint, Basile's conduct is indefensible. He systematically diverted Fusion-io e-mails and other information away from Fusion-io's computers that he sent and received as CEO for his own benefit and to the detriment of Fusion-io. That conduct is prohibited by the CFAA.

Basile argues that the interpretation proffered by Fusion-io would potentially criminalize an employee's use of her employer's computers for personal Christmas shopping. (*See* Memo. at 13.) Not so. Unlike giving a competitor access to confidential information stored on a company's computers or destroying that information, shopping for Christmas gifts is not antithetical to the employer's interests and, therefore, does not abrogate the employee's authorization to use the computers. Moreover, it does not impair the integrity or availability of the employer's information, so it does not cause damage within the meaning of the statute. Fusion-io is confident that, under the majority interpretation that it follows, courts have been and will be able to distinguish between an employee who uses a company's computers for incidental personal use, on the one hand, and an employee who uses a company's computers to engage in unfair competition with his or her employer, on the other. By contrast, Basile's interpretation of the CFAA protects only against purely hypothetical concerns and would cause very real problems – under his interpretation, courts would be powerless to remedy malicious destruction of data, transmission of viruses, initiation of denial-of-service attacks, and any number of other forms of statutorily-defined damage that employees could intentionally inflict on their employers.

Because Basile's interpretation of the CFAA would lead to absurd results and undermine Congress' intent in enacting the CFAA (as expressed in the plain language and legislative history of the statute), it should be rejected.

### C. **The Court Has Clear Supplemental Jurisdiction Over Fusion-io's State-Law Claims.**

Basile argues that if the Court dismisses "all claims over which it has original jurisdiction" – i.e., all three of Fusion-io's claims under the CFAA – then it has discretion also to dismiss Fusion-io's claims under state law. (Memo. at 17-18.) For the reasons set forth above, Fusion-io maintains that it has validly pled all three of its claims under the CFAA. At a bare minimum, however, it is absolutely clear that Fusion-io has pled at least one valid federal claim. While there is a split of authority (at least at the district court level) as to whether Fusion-io can maintain its Sixth and Seventh Claims against Basile, the authorities uniformly hold that Fusion-io can maintain its Fifth Claim against Basile. Therefore, Basile's motion to dismiss Fusion-io's state law claims should be denied.

## **CONCLUSION**

For the foregoing reasons, the Court should deny Basile's Motion to Dismiss Plaintiff's Complaint.

DATED this 29th day of May, 2009.

/s/ Scott S. Bell
DAVID M. BENNION
SCOTT S. BELL
PARSONS BEHLE & LATIMER
Attorneys for Plaintiff Fusion Multisystems, Inc., d/b/a Fusion-io

## CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on the 29th day of May, 2009, he electronically filed the foregoing **MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT** with the Clerk of the Court using the CM/ECF system, which sent electronic notice to the following:

Patricia Christensen
pchristensen@parrbrown.com

D. Craig Parry
cparry@parrbrown.com

/s/ Scott S. Bell